B. AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for preventing malicious network attacks said method comprising:

receiving a packet from a client computer;

identifying the client computer by a source IP address;

calculating a number of packets received using the source IP address during a time interval, wherein the calculating includes:

identifying a client data area based on the source IP address, the client data area including the number of packets received; and

incrementing the number of packets received;

comparing the number of packets received with one or more configuration settings;

determining an action from a plurality of actions based on the comparing; and

executing the action.

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Original) The method described in claim 1 further comprising:

receiving a socket request from the client computer;

PAGE 6/18 * RCVD AT 8/30/2005 4:57:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/27 * DNIS:2738300 * CSID:512 301 6742 * DURATION (mm-ss):04-54

determining a number of sockets opened for the client computer;

comparing the number of sockets opened to a socket limit; and

determining whether to allow a socket request based on the comparison.

6. (Canceled)

7. (Previously Presented) The method described in claim 1 further comprising:

providing a test script, the test script including one or more attack simulations;

processing the attack simulations included in the test script;

determining whether to change one or more of the configuration settings based on the processing; and

changing one or more of the configuration settings based on the determination.

8. (Currently Amended) An information handling system comprising:

one or more processors;

a memory accessible by the processors;

one or more nonvolatile storage devices accessible by the processors;

a network interface for receiving packets from a computer network; and

PAGE 7/18 * RCVD AT 8/30/2005 4:57:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/27 * DNIS:2738300 * CSID:512 301 6742 * DURATION (mm-ss):04-54

a packet handling tool to manage packets received from the network interface, the packet handling tool including:

means for receiving a packet from a client computer through the network interface;

means for identifying the client computer by a source IP address;

means for calculating a number of packets received using the source IP address during a time interval, wherein the means for calculating includes:

means for identifying a client data area based on the source IP address, the client data area including the number of packets received; and

means for incrementing the number of packets received;

means for comparing the number of packets received with one or more configuration settings;

means for determining an action from a plurality of actions based on the comparing; and

means for executing the action.

9. (Canceled)

10. (Canceled)

11. (Original) The information handling system as described in claim 8 further comprising:

means for receiving a socket request from the client computer;

PAGE 8/18 * RCVD AT 8/30/2005 4:57:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/27 * DNIS:2738300 * CSID:512 301 6742 * DURATION (mm-ss):04-54

means for determining a number of sockets opened for the client computer;

means for comparing the number of sockets opened to a socket limit; and

means for determining whether to allow a socket request based on the comparison.

12. (Canceled)

13. (Previously Presented) The information handling system as described in claim 8 further comprising:

means for providing a test script, the test script including one or more attack simulations;

means for processing the attack simulations included in the test script;

means for determining whether to change one or more of the configuration settings based on the processing; and

means for changing one or more of the configuration settings based on the determination

14. (Currently Amended) A computer program product for preventing malicious network attacks, said computer program product comprising:

means for receiving a packet from a client computer;

means for identifying the client computer by a source IP address;

means for calculating a number of packets received using the source IP address during a time interval, wherein the means for calculating includes:

PAGE 9/18 * RCVD AT 8/30/2005 4:57:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/27 * DNIS:2738300 * CSID:512 301 6742 * DURATION (mm-ss):04-54

means for identifying a client data area based on the source IP address, the client data area including the number of packets received; and

means for incrementing the number of packets received;

means for comparing the number of packets received with one or more configuration settings;

means for determining an action from a plurality of actions based on the comparing; and

means for executing the action.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Original) The computer program product described in claim 14 further comprising:

means for receiving a socket request from the client computer;

means for determining a number of sockets opened for the client computer;

means for comparing the number of sockets opened to a socket limit; and

means for determining whether to allow a socket request based on the comparison.

19. (Canceled)

20. (Previously Presented) The computer program product described in claim 18 further comprising:

means for providing a test script, the test script including one or more attack simulations;

means for processing the attack simulations included in the test script;

means for determining whether to change one or more of the configuration settings based on the processing; and

means for changing one or more of the configuration settings based on the determination.

21. (Previously Presented) The method of claim 1 wherein the configuration settings include a first limit and a second limit, the method further comprising:

determining that the number of packets exceeds the first limit;

sending a notification in response to determining that the number of packets exceeds the first limit;

receiving a subsequent packet from the client computer;

incrementing the number of packets in response to receiving the subsequent packet;

determining that the incremented number of packets exceeds the second limit; and

rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit.

22. (Previously Presented) The method of claim 1 wherein the configuration settings include a historical usage corresponding to the client computer, the method further comprising:
determining that the number of packets is higher than the historical usage; and
sending a notification in response to determining that the number of packets is higher than the historical usage.

23. (Previously Presented) The information handling system of claim 8 wherein the configuration settings include a first limit and a second limit, the information handling system further comprising:

means for determining that the number of packets exceeds the first limit;

means for sending a notification in response to determining that the number of packets exceeds the first limit;

means for receiving a subsequent packet over the network interface from the client computer;

means for incrementing the number of packets in response to receiving the subsequent packet;

means for determining that the incremented number of packets exceeds the second limit; and

means for rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit.

PAGE 12/18 * RCVD AT 8/30/2005 4:57:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/27 * DNIS:2738300 * CSID:512 301 6742 * DURATION (mm-ss):04-54

24. (Previously Presented) The information handling system of claim 8 wherein the configuration settings include a historical usage corresponding to the client computer, the information handling system further comprising:
means for determining that the number of packets is higher than the historical usage; and
means for sending a notification in response to determining that the number of packets is higher than the historical usage.

25. (Previously Presented) The computer program product of claim 14 wherein the configuration settings include a first limit and a second limit, the computer program product further comprising:

means for determining that the number of packets exceeds the first limit;

means for sending a notification in response to determining that the number of packets exceeds the first limit;

means for receiving a subsequent packet from the client computer;

means for incrementing the number of packets in response to receiving the subsequent packet;

means for determining that the incremented number of packets exceeds the second limit; and

means for rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit.

PAGE 13/18 * RCVD AT 8/30/2005 4:57:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/27 * DNIS:2738300 * CSID:512 301 6742 * DURATION (mm-ss):04-54

26. (Previously Presented) The computer program product of claim 14 wherein the configuration settings include a historical usage corresponding to the client computer, the computer program product further comprising:
means for determining that the number of packets is higher than the historical usage; and
means for sending a notification in response to determining that the number of packets is higher than the historical usage.

27 (Previously Presented) A method for preventing malicious network attacks on a server computer from a client computer that accesses the server computer via a computer network, said method comprising:

executing a test script that includes one or more attack simulations from the client computer, the execution of the test script including:

receiving, at the server computer, one or more packets from the client computer and one or more open socket requests from the client computer;

deciding a packet threshold for the client computer, the deciding including:

determining a number of packets received from the client computer during a time interval;

incrementing the number of packets received from the client computer; and

comparing the number of packets received with a packet limit stored at the server computer;

PAGE 14/18 * RCVD AT 8/30/2005 4:57:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/27 * DNIS:2738300 * CSID:512 301 6742 * DURATION (mm-ss):04-54

computing an open socket threshold for the client computer, the computing including:

determining a number of opened sockets for the client computer;

incrementing the number of opened sockets for the client computer;

comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and

evaluating the packet limit and the socket limit used during the attack simulations, the evaluating including:

analyzing the performance of the server computer during the simulation; and

adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from a group consisting the stored packet limit and the stored socket limit.